日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１２月２５日

出 願 番 号
Application Number: 平成１０年特許願第３７０９９２号

出 願 人
Applicant (s): 松下電器産業株式会社

１９９９年 ４月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０２１７３４

【書類名】　特許願

【整理番号】　2907707551

【提出日】　平成10年12月25日

【あて先】　特許庁長官　伊佐山　建志　殿

【国際特許分類】　G09C　1/00

【発明の名称】　ＥＴＣ認証システム及び認証方法

【請求項の数】　8

【発明者】

【住所又は居所】　神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

【氏名】　川崎　晃久

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代表者】　森下　洋一

【代理人】

【識別番号】　100099254

【弁理士】

【氏名又は名称】　役　昌明

【代理人】

【識別番号】　100100918

【弁理士】

【氏名又は名称】　大橋　公治

【代理人】

【識別番号】　100105485

【弁理士】

【氏名又は名称】　平野　雅典

【代理人】

【識別番号】　100108729

【弁理士】

【氏名又は名称】　林　紘樹

【手数料の表示】

【予納台帳番号】　037419

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9102150

【包括委任状番号】　9116348

【包括委任状番号】　9600935

【包括委任状番号】　9700485

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ＥＴＣ認証システム及び認証方法

【特許請求の範囲】

【請求項１】　路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、

前記伝達されたレスポンスデータを３分割する分割手段と、前記分割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段と、ＩＣカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、

前記路側機で生成したチャレンジデータを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、

前記路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証システム。

【請求項２】　路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由でＩＣカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化したデータを格納する段階と、格納された上記データの外にＩＣカードＩＤとＩＣカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で路側機に伝達する段階と、前記路側機において前記伝達されたレスポンスデータを３分割する段階と、前記分割されたＩＣカード個別鍵証明書データを検

証鍵に基づいて復号する段階と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する段階と、中央処理装置において前記路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証方法。

【請求項３】　第１の路側機を通過する直前にＩＣカードＩＤを送出するＩＤ送出手段と、第１の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で第２の路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、

前記レスポンスデータを３分割する第１の分割手段と、前記第１の分割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段とを備える第２の路側機と、

前記第１の路側機で生成したチャレンジデータとＩＣカードＩＤを分割する第２の分割手段と、前記第２の路側機で復号処理したチャレンジデータとＩＣカードＩＤを分割する第３の分割手段と、前記第２および第３の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、

前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第２の路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証システム。

【請求項４】　前記第２の路側機は、前記復号手段の復号の結果で取り出されたＩＣカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化デー

タを復号処理する別の復号手段と、該復号手段の復号の結果により前記第１の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する確認手段と、を更に含むことを特徴とする請求項３記載のＥＴＣ認証システム。

【請求項５】　第１の路側機を通過する直前に車載機経由でＩＣカードからのカードＩＤを受信する段階と、前記第１の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由でＩＣカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外にＩＣカードＩＤとＩＣカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第２の路側機に伝達する段階と、前記第２の路側機において前記伝達されたレスポンスデータを３分割する段階と、前記分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する段階と、中央処理装置において前記第１の路側機から得たチャレンジデータと前記第２の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証方法。

【請求項６】　前記復号処理の段階で取り出されたＩＣカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化データを復号処理する段階と、該復号処理の復号の結果により前記第１の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する段階を更に含むことを特徴とする請求項５記載のＥＴＣ認証方法。

【請求項７】　第１の路側機を通過する直前にＩＣカードＩＤを送出するＩＤ送出手段と、第１の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で

第２の路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、

前記レスポンスデータを３分割する第１の分割手段と、前記第１の分割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段とを備える第２の路側機と、

前記第１の路側機で生成したチャレンジデータとＩＣカードＩＤを分割する第２の分割手段と、前記第２の路側機で復号処理したチャレンジデータとＩＣカードＩＤを分割する第３の分割手段と、前記第２および第３の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、

前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第２の路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証システム。

【請求項８】　第１の路側機を通過する直前に車載機経由でＩＣカードからのカードＩＤを受信する段階と、前記第１の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由でＩＣカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外にＩＣカードＩＤとＩＣカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第２の路側機に伝達する段階と、前記第２の路側機において前記伝達されたレスポンスデータを３分割する段階と、前記分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する段階と、中央処理装置において前記第１の路側機から得たチャレンジデータと前記第２の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はＥＴＣ（自動料金収受）認証システム及び認証方法に関し、特にＩＣカードの正当性を路側機および中央処理装置が直接認証しうるよう構成したものである。

【０００２】

【従来の技術】

従来のＥＴＣ認証システムは、システム上の制約から、路側機は車載機を認証し、車載機はＩＣカードを認証するという２段階認証を行なうものであり、路側機は間接的にしかＩＣカードを認証することができないという構成であった。

【０００３】

これを図４および図５を用いて説明する。図４は、ＩＣカードと車載機間の相互認証動作を説明するための図である。図４において、

（１）ＩＣカード41は車載機42にETCS鍵センタ発行のＩＣカード検証鍵証明書CERT－PICPとＩＣカード発行センタのＩＣカード個別鍵証明書CERT－KICCを送付する。

（２）車載機42はETCS鍵センタの検証鍵Ｐｃ１を用いてＩＣカード検証鍵証明書CERT－PICP から回復型署名検証Rverify（Ｐｃ１，CERT－PICP）によってＩＣカード発行センタの検証鍵ＰICPを取り出す。

（３）車載機42はＰICPを用いてＩＣカード個別鍵証明書CERT－KICCから回復型署名検証Rverify（PICC，CERT－KICC）によってＩＣカード個別鍵ＫICCを取り出す。一方、ＩＣカードによる車載機の認証のため、ＩＣカード発生の乱数Ｒ２をチャレンジとして車載機42に転送する。

（４）車載機42はセッション鍵Ks1を発生し、上記のように取り出したＩＣカード個別鍵ＫICCを用いて暗号化、すなわちE(KICC，Ks1)の処理を行なってＩＣカード41に返す。さらに上記乱数Ｒ２に対するレスポンスとして、暗号化したもの、すなわちE(Ks1,R1‖R2)をＩＣカード41に返す。ＩＣカード41がこれを復号した結果と発生した乱数Ｒ２と比較し、一致することにより車載機42を正当なも

のと認証し、続くトランザクションを続行する。一致しなければトランザクションを中断する。

（５）車載機42は、車載機発生の乱数Ｒ１をチャレンジとしてＩＣカード41に転送し、ＩＣカード41がこれに対してセッション鍵Ks2を用いて暗号化、すなわちE(Ks1, R1‖ Ks2)の処理を行なってレスポンスとして車載機42に返す。

（６）車載機42がこれに対しセッション鍵Ks1を用いて復号し、その結果と発生した乱数Ｒ１とを比較し、一致すればＩＣカード41を正当なものと認証し、トランザクションを続行する。一致しなければトランザクションを中断する。

【０００４】

このように認証のためのプロトコルを実行することにより、第１段階として、まずＩＣカード41と車載機42間の相互認証を実現する。次に、第２段階として、車載機と路側機間の相互認証について説明する。

【０００５】

図５は、車載機と路側機間の相互認証動作を説明するための図である。図５において、

（１）車載機51は車載機個別鍵証明書CERT－ＫOBEと個別鍵ＫOBEを鍵として乱数Ｋを暗号化、すなわちＥ(KOBE, K)処理をしたものを路側機52に配送する。

（２）路側機52はETCS鍵センタの署名検証鍵Ｐｃ２により車載機個別鍵証明書CERT－ＫOBEから次の式によりＯＢＥＩＤ‖ＫOBEを取り出す。

Ｘ＝c1Ｐ＋c2Ｑ＝ＯＢＥＩＤ‖ＫOBE

（３）車載機51は車載機で生成したチャレンジデータＫを路側機52に送り、路側機52がＫOBEを用いて正しく復号できることを確認することにより路側機52を認証する

（４）路側機52は路側機で生成したチャレンジデータR2をＫOBEを用いて暗号化、すなわちＥ(ＫOBE, Ｋ‖R2)し、車載機51がこれを復号できることを確認することにより車載機51を認証する。

【０００６】

【発明が解決しようとする課題】

このように従来のＥＴＣ認証システムは、路側機は車載機を認証し、車載機は

ＩＣカードを認証するという２段階認証を行なうものであり、路側機は間接的にしかＩＣカードを認証できないので、従来方式は、路側機の下を通過するときにＩＣカードと路側機とで直接的にデータのやり取りができないという問題を有していた。また、２段階認証を行なうので、システムが複雑で高価なものにならざるを得ないという問題も有していた。

【０００７】

そこで、本発明は、ＩＣカードの正当性を路側機および中央処理装置が直接的に認証することができるＥＴＣ認証システム及び認証方法を提供することを目的とするものである。

【０００８】

【課題を解決するための手段】

本発明によるＥＴＣ認証システムは、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、前記伝達されたレスポンスデータを３分割する分割手段と、前記分割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段と、ＩＣカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、前記路側機で生成したチャレンジデータを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とす

る。

【０００９】

このような構成とすることにより本発明は、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができる。

【００１０】

【発明の実施の形態】

本発明の請求項１記載の発明は、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、前記伝達されたレスポンスデータを３分割する分割手段と、前記分割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段と、ＩＣカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、前記路側機で生成したチャレンジデータを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証システムとしたものであり、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカード

のＩＤを直接認証することができるという作用を有する。

【００１１】

また、請求項２記載の発明は、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由でＩＣカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化したデータを格納する段階と、格納された上記データの外にＩＣカードＩＤとＩＣカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で路側機に伝達する段階と、前記路側機において前記伝達されたレスポンスデータを３分割する段階と、前記分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する段階と、中央処理装置において前記路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証方法としたものであり、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができるという作用を有する。

【００１２】

また、請求項３記載の発明は、第１の路側機を通過する直前にＩＣカードＩＤを送出するＩＤ送出手段と、第１の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で第２の路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、前記レスポンスデータを３分割する第１の分割手段と、前記第１の分割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前

記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段とを備える第２の路側機と、前記第１の路側機で生成したチャレンジデータとＩＣカードＩＤを分割する第２の分割手段と、前記第２の路側機で復号処理したチャレンジデータとＩＣカードＩＤを分割する第３の分割手段と、前記第２および第３の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第２の路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証システムとしたものであり、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができるという作用を有する。

【００１３】

また、請求項４記載の発明は、前記第２の路側機は、前記復号手段の復号の結果で取り出されたＩＣカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化データを復号処理する別の復号手段と、該復号手段の復号の結果により前記第１の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する確認手段と、を更に含むことを特徴とする請求項３記載のＥＴＣ認証システムとしたものであり、通過に要した時間が正しいか否かをと判定し、正しくない場合には、不正通行として、ＩＣカードＩＤをネガリストに載せることができるという作用を有する。

【００１４】

また、請求項５記載の発明は、第１の路側機を通過する直前に車載機経由でＩＣカードからのカードＩＤを受信する段階と、前記第１の路側機を通過した際に当該路側機で生成したチャレンジデータと現在時刻を車載機経由でＩＣカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外にＩＣカードＩＤとＩＣカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第２の路側機に伝達する段階と、前記第２の路側機において前記

伝達されたレスポンスデータを３分割する段階と、前記分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する段階と、中央処理装置において前記第１の路側機から得たチャレンジデータと前記第２の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証方法としたものであり、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができるという作用を有する。

【００１５】

また、請求項６記載の発明は、前記復号処理の段階で取り出されたＩＣカード個別の秘密鍵を基に前記分割されて取り出された前記暗号化データを復号処理する段階と、該復号処理の復号の結果により前記第１の路側機を通過した際の現在時刻情報を取り出し、この時刻情報と現在時刻との差が所定時間内のものであるか否かを確認する段階を更に含むことを特徴とする請求項５記載のＥＴＣ認証方法としたものであり、通過に要した時間が正しいか否かをと判定し、正しくない場合には、不正通行として、ＩＣカードＩＤをネガリストに載せることができるという作用を有する。

【００１６】

また、請求項７記載の発明は、第１の路側機を通過する直前にＩＣカードＩＤを送出するＩＤ送出手段と、第１の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化されたデータとをレスポンスデータとして前記車載機経由で第２の路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、前記レスポンスデータを３分割する第１の分割手段と、前記第１の分

割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段とを備える第２の路側機と、前記第１の路側機で生成したチャレンジデータとＩＣカードＩＤを分割する第２の分割手段と、前記第２の路側機で復号処理したチャレンジデータとＩＣカードＩＤを分割する第３の分割手段と、前記第２および第３の分割手段から得たチャレンジデータの一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記第２の路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証システムとしたものであり、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができるという作用を有する。

【００１７】

また、請求項８記載の発明は、第１の路側機を通過する直前に車載機経由でＩＣカードからのカードＩＤを受信する段階と、前記第１の路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由でＩＣカードに伝達し、それを正規の秘密鍵で暗号化する段階と、暗号化されたデータの外にＩＣカードＩＤとＩＣカード個別鍵証明書の各データをレスポンスデータとして前記車載機経由で第２の路側機に伝達する段階と、前記第２の路側機において前記伝達されたレスポンスデータを３分割する段階と、前記分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号する段階と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する段階と、中央処理装置において前記第１の路側機から得たチャレンジデータと前記第２の路側機で復号したチャレンジデータの一致判定を行なう段階とを含み、前記第２の路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデ

ータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするＥＴＣ認証方法としたものであり、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができるという作用を有する。

【００１８】

以下、本発明の実施の形態について、図面に基づき説明する。

【００１９】

（第１の実施の形態）

図１は、本発明の第１の実施形態のＥＴＣ認証システムを説明するための図であり、第１の実施形態のＥＴＣ認証システムは、ＩＣカードの直接動的一方向認証（チャレンジレスポンス）を行なうものである。

【００２０】

図１において、料金所路側機13を通過する際、ＩＣカード11に記憶されたレスポンスデータ、すなわち料金所路側機13を通過した際に当該路側機13で生成した乱数(RND)がチャレンジデータとして車載機12経由でＩＣカード11に伝送され、それを正規の秘密鍵Ｋiccで暗号化したもの、が料金所路側機13に送信される。この際、ＩＣカード11のＩＤ(ICCID)とＩＣカード個別鍵証明書CERT－Ｋiccが共に送信される。

【００２１】

路側機13では、送られてきたデータを３つに分割、すなわちレスポンスデータであるＥ(Ｋicc, RND)と、ICCIDと、ＩＣカード個別鍵証明書CERT－Ｋiccに分割する。

【００２２】

次にＩＣカード個別鍵証明書CERT－Ｋicc を検証鍵PCに基づいて復号処理(ＤＥＣ)すると、ＫiccとICCIDという情報を取り出すことができる。このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればＩＣカードＩＤの署名確認を行なうことができる。その結果、ＩＣカード個別鍵証明書CERT－Ｋiccが正しいということが判るので、一緒に取り出したＫicc

も正しいということが判る。そしてこのKiccを鍵として最初に送ろうとしていたレスポンスデータ、すなわち暗号処理されたE(Kicc, RND)を復号処理(ＤＥＣ)して、料金所路側機13で生成したチャレンジデータ、すなわち乱数(ここではRND')を取り出す。

【００２３】

このデータは上記したICCIDと結合されて料金所路側機13からセンター装置14に送られ、センター装置14において上記したRND'を再度取り出し、料金所路側機13からの乱数RNDをＩＣカード11に記憶の際にセンター装置14にも送られてそれを記憶しておいた乱数RNDを取り出して一致判定を行なう。

【００２４】

その結果、センター装置14において同じICCIDを持つ乱数RNDと乱数RND'が一致することで、ＩＣカード11は正規の秘密鍵Kiccを持つことが確認できるので、路側機センター装置14としてＩＣカードＩＤを動的にかつ一方向的に直接認証することができる。

【００２５】

なお、この動作と並行して、料金所路側機13で生成されたチャレンジデータ(乱数RND)は、車載機12が料金所を通過した時点で料金所路側機13から車載機12へ渡される。この乱数RNDは車載機12と料金所路側機13との間の所定の通信手順(ＤＳＲＣ)の終了後に車載機13からＩＣカード11へ送られ、ＩＣカード11にて暗号化、すなわちE(Kicc, RND)の処理がなされる。暗号化されたデータはレスポンスデータとしてＩＣカード11に記憶される。

【００２６】

(第２の実施の形態)

図２は、本発明の第２の実施形態のＥＴＣ認証システムを説明するための図であり、第２の実施形態のＥＴＣ認証システムは、同一料金所の予告路側機と路側機を組合わせることで、上記第１の実施形態と同様にＩＣカードの直接動的認証を行なうものである。

【００２７】

図２において、料金所の手前、例えば30m、に設けられた予告路側機24を通過

する際、ＩＣカード21に記憶されているＩＤ(ICCID)が車載機22経由で予告路側機24に送信される。予告路側機24では、ＩＣカード21から送られてきたICCIDと予告路側機24で生成されている乱数(RND)と現在時刻(Time)を組み合わせて一方はＩＣカード21に、他方は車線装置25に送信する。

【００２８】

ＩＣカード21では、受け取ったデータのうち、乱数(RND)および現在時刻(Time)のデータに対して正規の秘密鍵Ｋiccで暗号化、すなわちＥ(Ｋicc, Time‖RND)を施したものが、予告路側機24から料金所に移動する間に実行される。そして、ＩＣカード21のＩＤ(ICCID)およびＩＣカード個別鍵証明書CERT－Ｋiccと一緒に料金所路側機23に送信される。

【００２９】

料金所路側機23では、送られてきたデータを３つに分割、すなわちＥ(Ｋicc, Time‖RND)と、ICCIDと、ＩＣカード個別鍵証明書CERT－Ｋiccに分割する。

【００３０】

次にＩＣカード個別鍵証明書CERT－Ｋicc を検証鍵PCに基づいて復号処理(ＤＥＣ)すると、ＫiccとICCIDという情報を取り出すことができる。このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればＩＣカードＩＤの署名確認を行なうことができる。その結果、ＩＣカード個別鍵証明書CERT－Ｋiccが正しいということが判るので、一緒に取り出したＫiccも正しいということが判る。そしてこのＫiccを鍵として暗号処理されたＥ(Ｋicc, Time‖RND)を復号処理(ＤＥＣ)して、予告路側機24で生成した乱数(ここではRND’)および現在時刻(ここではTime’)を取り出す。

【００３１】

取り出した現在時刻(ここではTime’)と、予告路側機24を通過する時点の現在時刻(Time)との差を取り、その値が所定の値(例えばｎ分)以内であれば通過に要した時間が正しいと判定し、また所定の値(例えばｎ分)を越えていれば、通過に要した時間が正しくないと判定し、不正通行として、ＩＣカードＩＤをネガリストに載せることができる。

【００３２】

同じく取り出した乱数(ここではRND')は、上記したように分割して取り出したICCIDと結合されて料金所路側機23から車線装置25に送られ、車線装置25において上記したRND'を再度取り出し、既に予告路側機24から車線装置24に送られている乱数(RND)を取り出して一致判定を行なう。

【００３３】

その結果、車線装置24において同じICCIDを持つ、乱数RNDと乱数RND'が一致することとなり、その結果、ＩＣカード21は正規の秘密鍵Ｋiccを持つことが確認できるので、車線装置25としてＩＣカードＩＤを直接動的に認証することができる。

【００３４】

（第３の実施の形態）

図３は、本発明の第３の実施形態のＥＴＣ認証システムを説明するための図であり、第３の実施形態のＥＴＣ認証システムは、入口料金所路側機と出口路側機を組合わせることで、上記第２の実施形態と同様にＩＣカードの直接動的認証を行なうものである。

【００３５】

図３において、ＩＣカード31が挿入された車載機32が入口料金所路側機34の下を通ると、ＩＤカード31と入口料金所路側機34とでデータのやりとりが行なわれる。すなわち、ＩＣカード31からカードＩＤ(ICCID)が料金所路側機34に送られると、料金所路側機34はチャレンジデータとしての乱数(RND)を生成し、料金所路側機34からＩＣカード31に乱数(RND)を送る。

【００３６】

同時に、入口料金所路側機34は、カードＩＤ(ICCID)と乱数(RND)をセンター装置35に送信する。ここまでは、入口料金所路側機34を通過する間に処理が行なわれる。

【００３７】

この入口料金所路側機34を通過した後にＩＣカード31の中では、次の料金所、すなわち出口料金所路側機33を通るまでに、いま受け取った乱数(RND)に対して暗号処理(ＥＮＣ)、すなわちＥ(Ｋicc, RND)の処理を行なって、暗号結果を格納

する。

【００３８】

その結果、ＩＣカード31では、暗号化されたデータが格納されたことになるので、次に車載機32に挿入されたＩＣカード31が出口料金所路側機33を通る時に既に暗号化されているデータを出口料金所路側機33に送信することができる。

【００３９】

その際には、暗号化されたデータだけでなく、ＩＣカードのＩＤ(ICCID)およびＩＣカード個別鍵証明書CERT－Ｋiccも送信する。これらのデータを出口路側機33で受け取り、Ｅ(Ｋicc, RND)と、ICCIDと、ＩＣカード個別鍵証明書CERT－Ｋicc の３つに分割する。

【００４０】

ＩＣカード個別鍵証明書CERT－Ｋicc を出口料金所路側機33が持っている検証鍵PCに基づいて復号処理(ＤＥＣ)すると、KiccとICCIDという情報を取り出すことができる。

【００４１】

このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればＩＣカードＩＤの署名確認を行なうことができる。一致することになると、ＩＣカード個別鍵証明書CERT－Ｋiccが正しいということが判るので、一緒に取り出したＫiccも正しいということが判る。そしてこのＫiccを鍵として暗号化データＥ(Ｋicc, RND)を復号処理(ＤＥＣ)して、最初に入口料金所路側機34で生成した乱数(ここではRND’)を取り出す。

【００４２】

取り出したデータは上記に分割して取り出したICCIDと結合されて出口料金所路側機33からセンター装置35に送られ、センター装置35において上記した乱数RND’を再度取り出し、既に入口料金所路側機34から送られ格納されている乱数RNDと比較し、一致判定を行なう。

【００４３】

その結果、センター装置35においては、入口と出口で取り出した同じICCIDを持つ、乱数RNDと乱数RND’の一致を判定できるので、ＩＣカード31が正規の秘密

鍵Ｋiccを持つものであることが確認でき、センター装置35としてＩＣカードＩＤを動的に認証することができる。

【００４４】

このように第３の実施形態は、入口料金所および出口料金所に２つの路側機を設置し、これらを組み合わせることにより乱数データをセンター装置に集めることができるので、直接動的にＩＣカードの認証を行なうことができる。

【００４５】

なお、以上の説明においては、正規の秘密鍵Ｋiccとしては、専ら公開鍵をもつ暗号方式すなわちＤＥＳ方式で使用されるものを念頭において説明したが、この公開鍵に限らず、他の暗号方式である楕円曲線暗号方式や、ＲＡＳなどの種々の暗号方式で使用される鍵であっても良いことは勿論である。

【００４６】

この場合、たとえば楕円曲線暗号方式の専用ＬＳＩを採用することにより、２アンテナ方式の入口料金所においても料金所通過時間内に、署名検証の処理が可能となる。

【００４７】

【発明の効果】

以上説明したように本発明のＥＴＣ認証システムは、路側機を通過した際に当該路側機で生成したチャレンジデータを車載機経由で受信し、それを正規の秘密鍵で暗号化する暗号化手段と、該暗号化手段によって暗号化したデータを格納する暗号化データ格納手段と、予めＩＣカードに付与されているＩＣカードＩＤ及びＩＣカード個別鍵証明書の各データと前記暗号化データ格納手段に格納されている暗号化されているデータとをレスポンスデータとして前記車載機経由で路側機に伝達するレスポンスデータ伝達手段とを備えるＩＣカードと、前記伝達されたレスポンスデータを３分割する分割手段と、前記分割手段により分割されたＩＣカード個別鍵証明書データを検証鍵に基づいて復号処理する復号手段と、復号の結果で取り出されたＩＣカードＩＤと前記で分割されて得られたＩＣカードＩＤを一致検出する一致検出手段と、ＩＣカードにチャレンジデータを伝達するチャレンジデータ送出手段とを備える路側機と、前記路側機で生成したチャレンジ

データを格納するチャレンジデータ格納手段と、前記路側機で復号処理したチャレンジデータを受信し、前記チャレンジデータ格納手段に格納してあるチャレンジデータと一致判定を行なう一致判定手段とを備える中央処理装置と、を含み、前記路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に前記中央処理装置にて前記路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことによりＩＣカードのＩＤの直接認証を行なうことを特徴とするものであり、路側機がＩＣカードＩＤと同時に受領した署名情報を、署名検証処理すると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができるという優れた効果を有する。

【００４８】

また、本発明のＥＴＣ認証システムは、路側機２台を使用し、第１の路側機から第２の路側機に移動する間に、ＩＣカードに対する書き込み処理を行ない、ＩＣカードに書き込まれたデータ(レスポンスデータ)を使って第２の路側機がＩＤカードのＩＤの認証を直接行なうことができると共に中央処理装置にて路側機が復号したＩＣカードで暗号化したチャレンジデータの一致判定を行なうことにより、ＩＣカードのＩＤを直接認証することができるという優れた効果を有する。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係るＥＴＣ認証システムを説明するためのブロック図、

【図２】

本発明の第２の実施形態に係るＥＴＣ認証システムを説明するためのブロック図、

【図３】

本発明の第３の実施形態に係るＥＴＣ認証システムを説明するためのブロック図、

【図４】

従来のＥＴＣ認証システムの一部であるＩＣカードと車載機間の相互認証動作

を説明するための図、

【図５】

従来のＥＴＣ認証システムの一部である車載機と路側機間の相互認証動作を説明するための図である。

【符号の説明】

11、21、31、41　ＩＣカード

12、22、32、42、51　車載機

13、23　料金所路側機

14、35　センター装置(中央処理装置)

24　予告路側機

25　車線装置(中央処理装置)

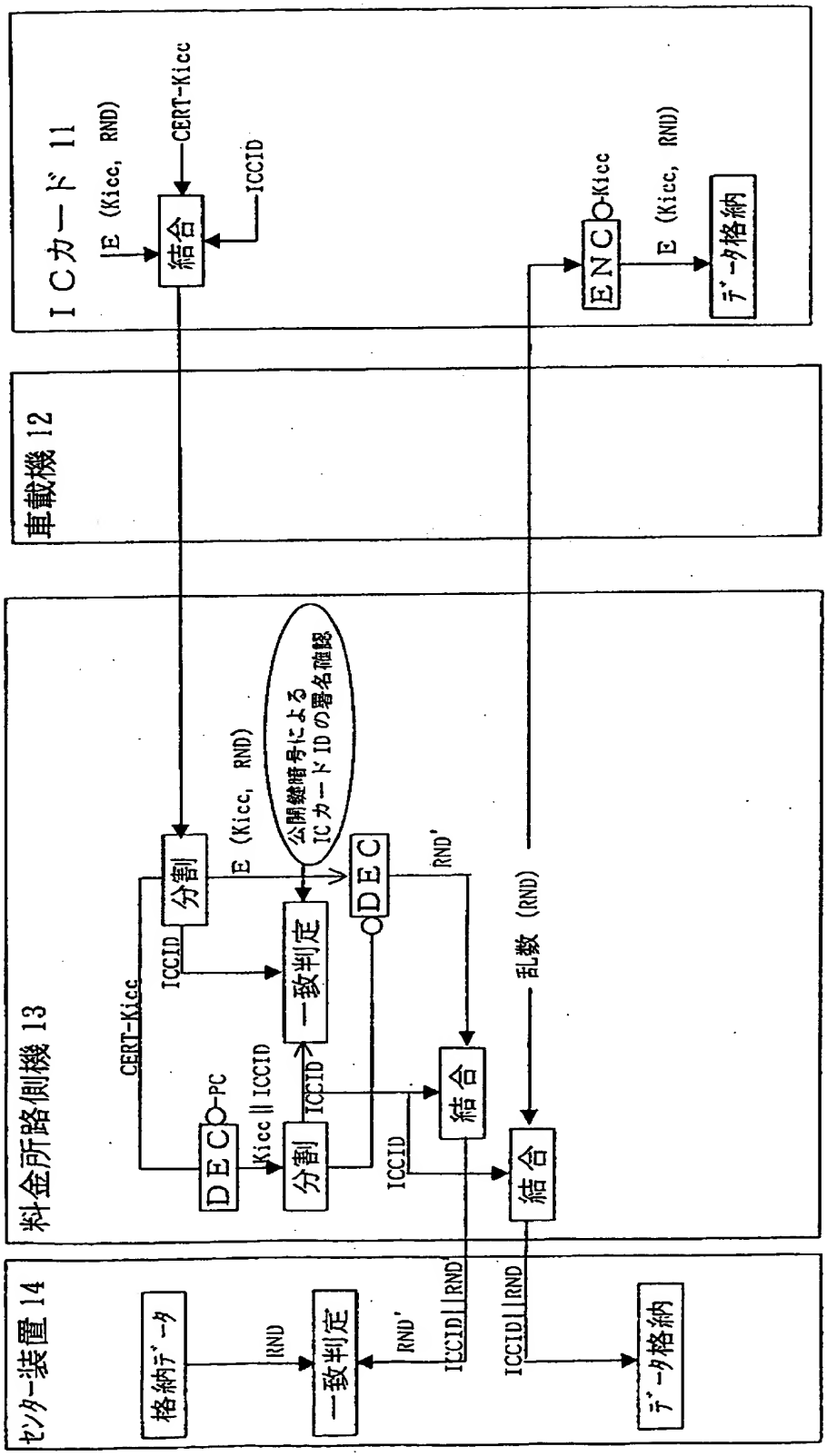
33　出口料金所路側機

34　入口料金所路側機

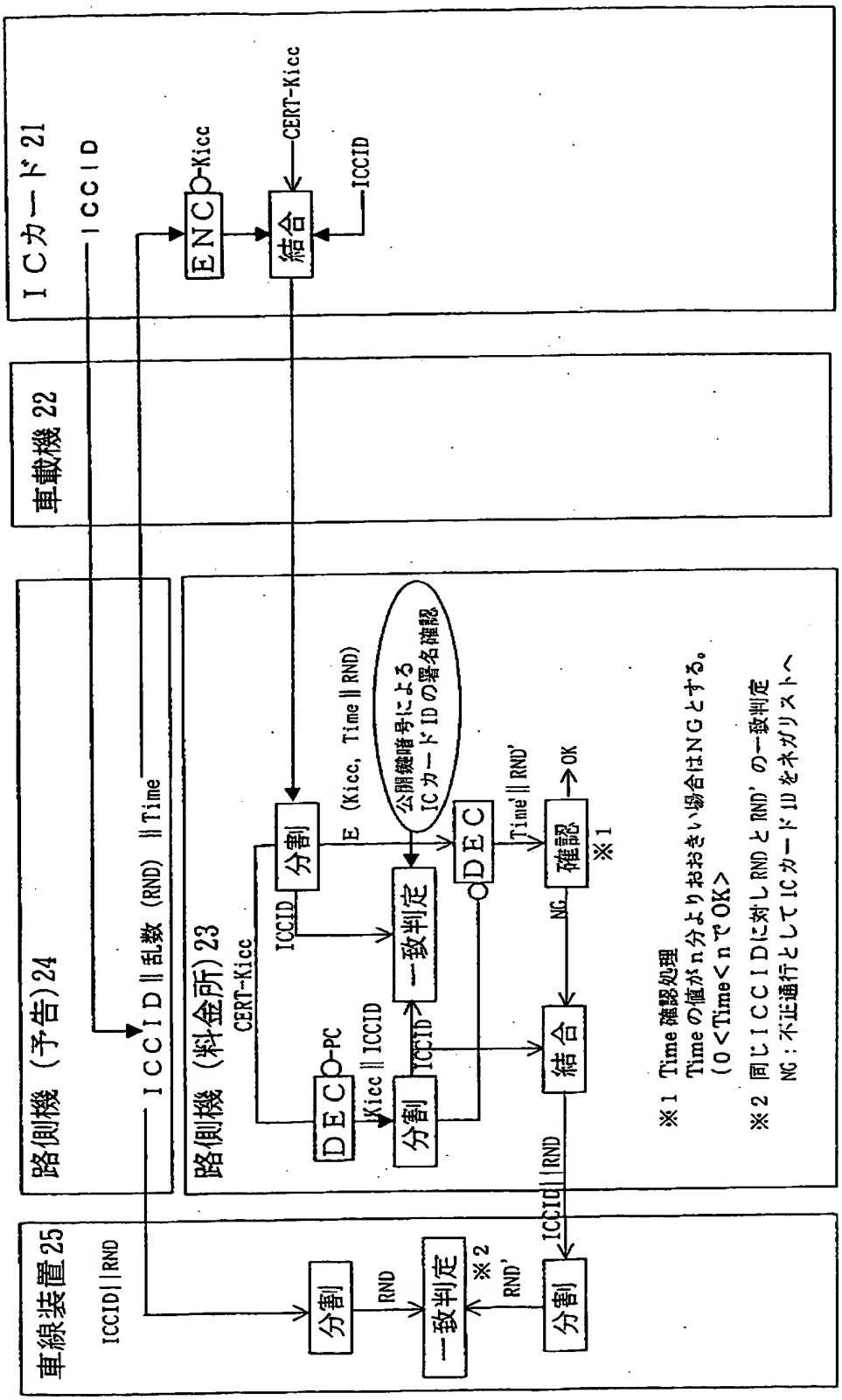
52　路側機

【書類名】　図面

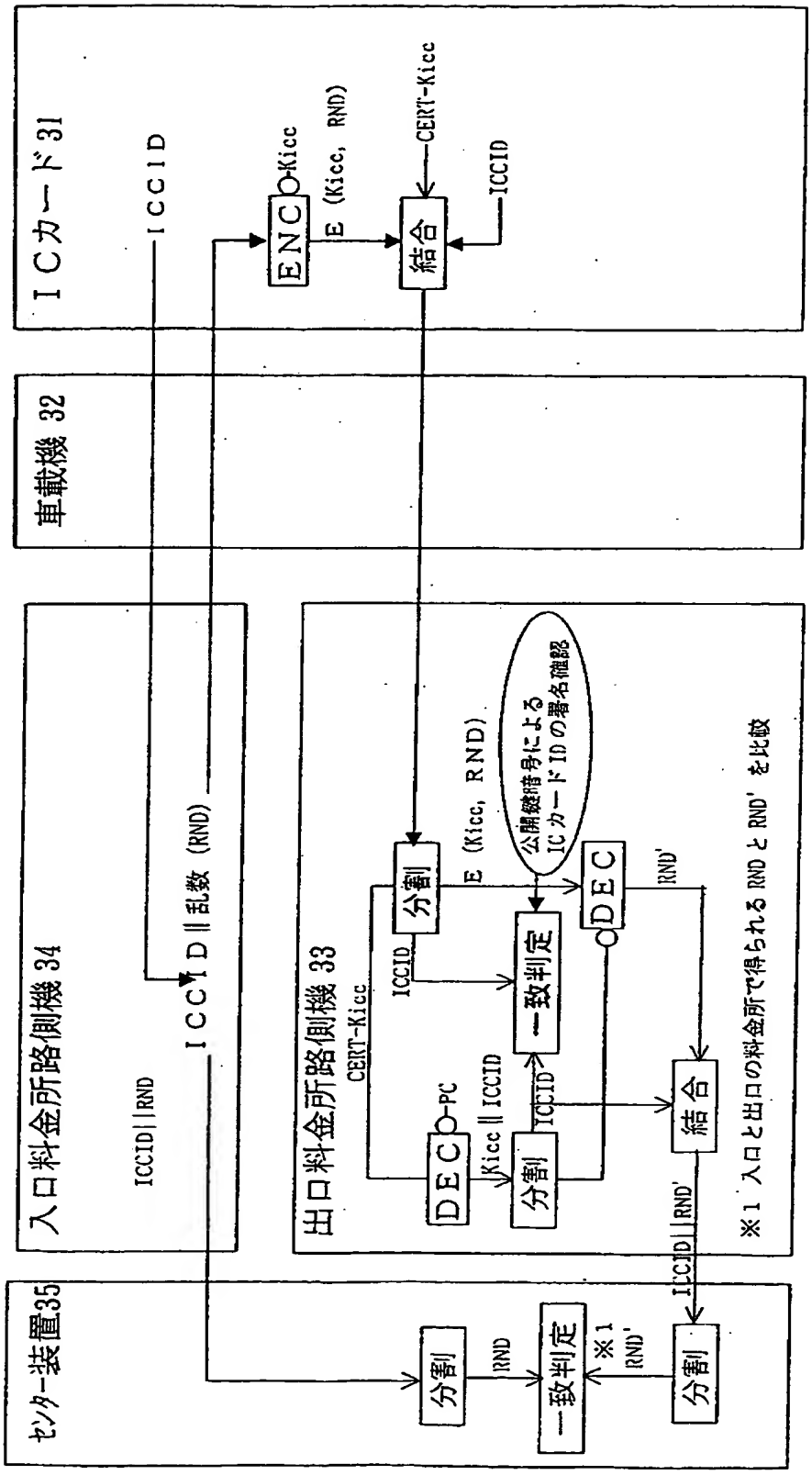
【図１】


ＩＣカード 11
E (Kicc, RND)
CERT-Kicc
ICCID
結合
ＥＮＣ
Kicc
E (Kicc, RND)
データ格納
車載機 12
料金所路側機 13
公開鍵暗号による
ICカードIDの署名確認
分割
E (Kicc, RND)
ICCID
CERT-Kicc
一致判定
ＤＥＣ
RND'
ＤＥＣ
PC
Kicc || ICCID
分割
ICCID
結合
乱数 (RND)
結合
センター装置 14
格納データ
RND
一致判定
RND'
ICCID || RND
ICCID || RND
データ格納

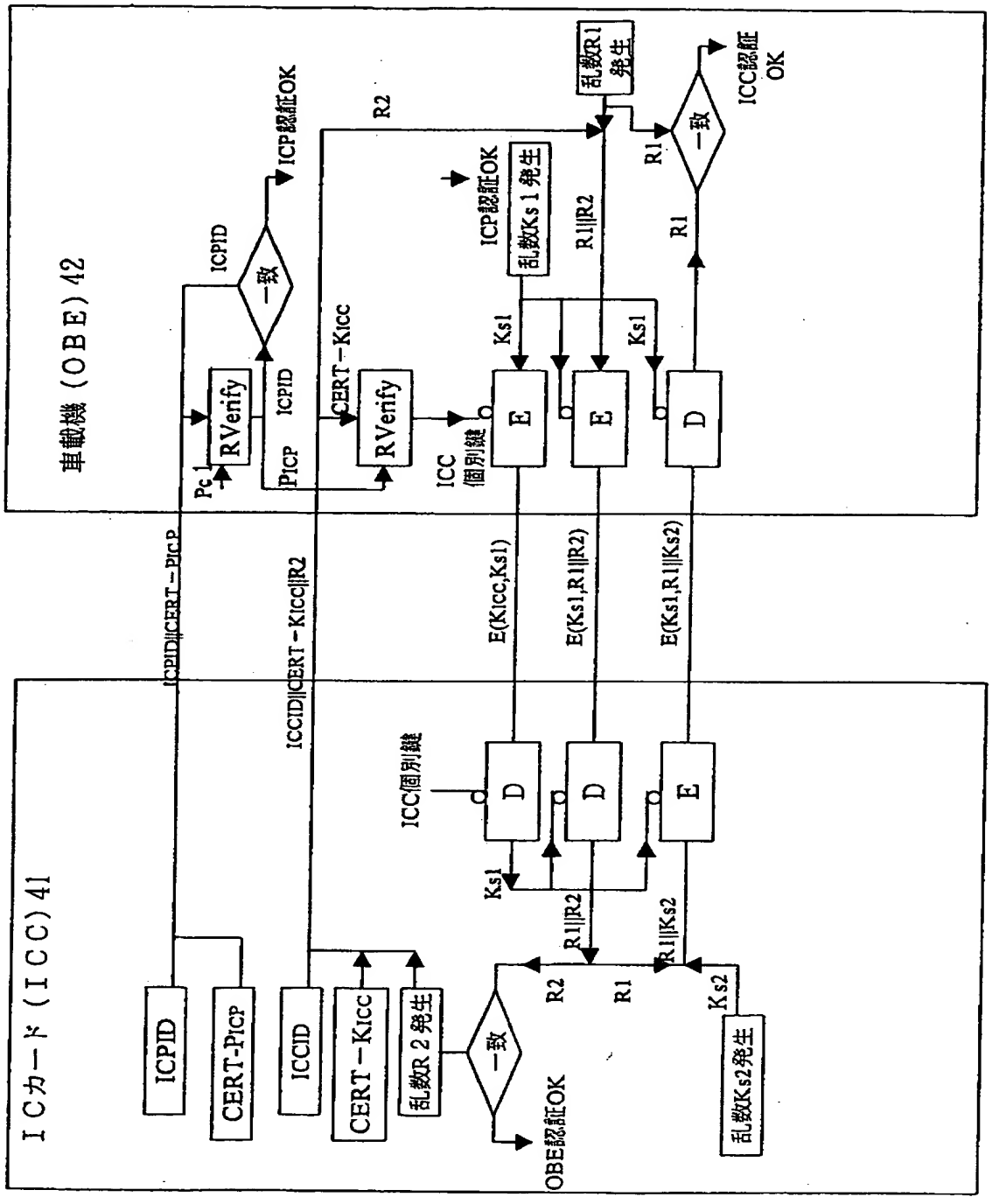
【図２】


ＩＣカード21
車載機 22
路側機（予告）24
路側機（料金所）23
車線装置 25
ＩＣＣＩＤ
ＥＮＣ
Kicc
結合
CERT-Kicc
ICCID
ＩＣＣＩＤ‖乱数（RND）‖Time
ICCID‖RND
分割
RND
一致判定
※２
RND'
ICCID‖RND
CERT-Kicc
ICCID
E（Kicc，Time‖RND）
公開鍵暗号による
ＩＣカードＩＤの署名確認
ＤＥＣ
Time'‖RND'
確認
※１
OK
NG
Kicc‖ICCID
ICCID
※１ Time確認処理
Timeの値がｎ分よりおおきい場合はＮＧとする。
（0＜Time＜ｎでOK）
※２ 同じＩＣＣＩＤに対しRNDとRND'の一致判定
NG：不正通行としてＩＣカードＩＤをネガリストへ

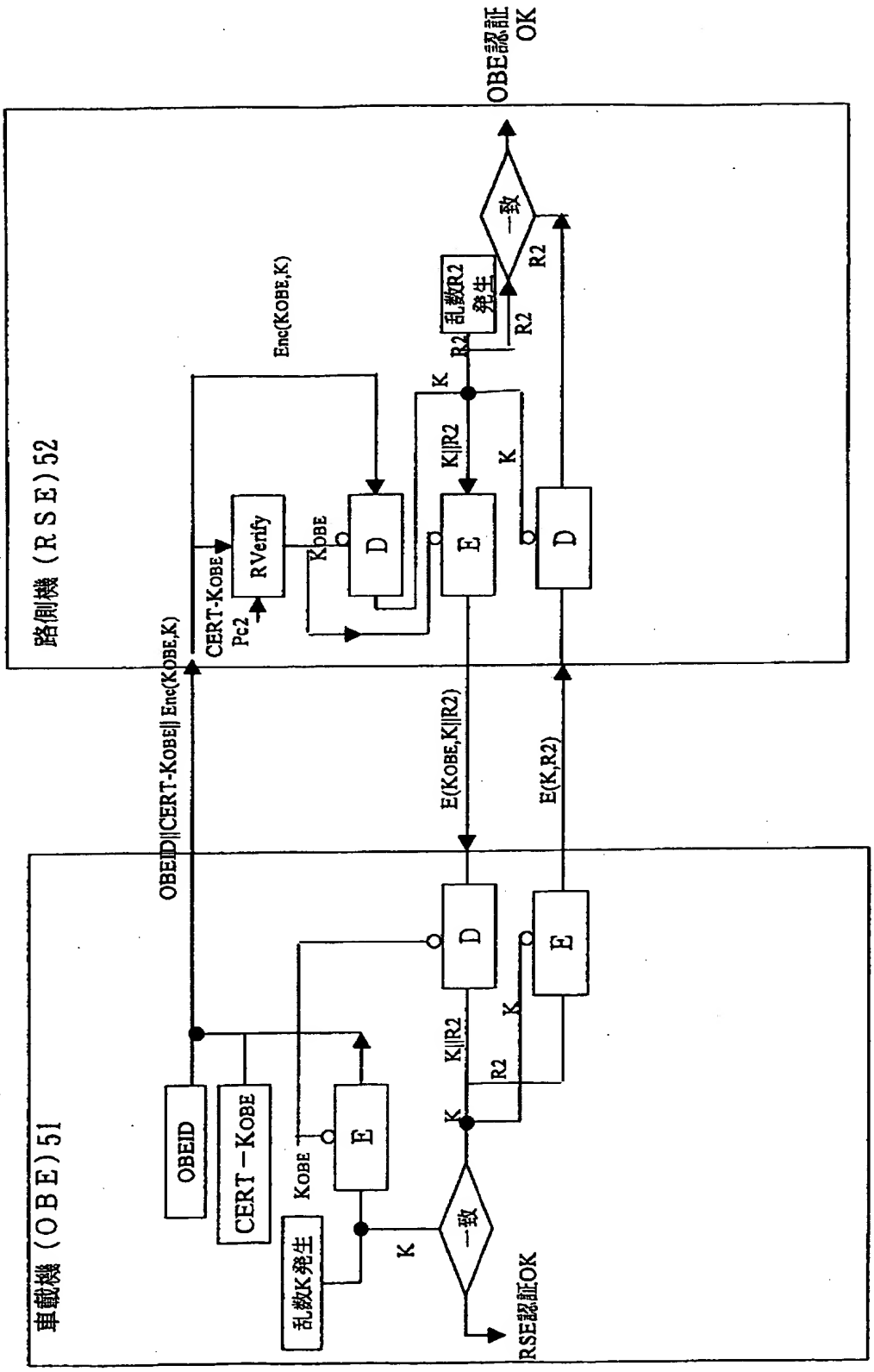
【図３】


ＩＣカード31
車載機 32
入口料金所路側機 34
出口料金所路側機 33
センター装置35
ＩＣＣＩＤ
ＥＮＣ
Kicc
Ｅ (Kicc, RND)
結合
CERT-Kicc
ICCID
ICCID||RND
ＩＣＣＩＤ‖乱数 (RND)
分割
Ｅ (Kicc, RND)
公開鍵暗号による
ICカードIDの署名確認
一致判定
ＤＥＣ
RND'
CERT-Kicc
ICCID
PC
Kicc‖ICCID
ICCID
結合
ICCID||RND'
※１ 入口と出口の料金所で得られるRNDとRND'を比較
分割
RND
一致判定
※1
RND'
分割

【図４】


車載機（ＯＢＥ）42
ICカード（ＩＣＣ）41
ICPID
CERT-PICP
ICCID
CERT－KICC
乱数R２発生
乱数Ks2発生
乱数R1発生
乱数Ks１発生
RVerify
RVerify
一致
一致
一致
ICP認証OK
ICP認証OK
ICC認証OK
OBE認証OK
ICC個別鍵
ICC個別鍵
E
E
D
D
D
E
Pc1
PICP
R1
R2
R1||R2
R1||Ks2
Ks1
Ks2
E(KICC,Ks1)
E(Ks1,R1||R2)
E(Ks1,R1||Ks2)
ICPID||CERT－PICP
ICCID||CERT－KICC||R2

【図５】


OBE認証 OK
路側機（ＲＳＥ）52
Enc(KOBE,K)
CERT-KOBE
Pc2
RVerify
KOBE
D
E
D
K
K||R2
K
乱数R2 発生
R2
R2
R2
一致
OBEID||CERT-KOBE|| Enc(KOBE,K)
E(KOBE,K||R2)
E(K,R2)
車載機（ＯＢＥ）51
OBEID
CERT－KOBE
KOBE
E
乱数K発生
K
一致
D
E
K||R2
K
R2
K
RSE認証OK

【書類名】　　要約書

【要約】

【課題】　ＩＣカードの正当性を路側機および中央処理装置が直接的に認証することができるＥＴＣ認証システム及び認証方法を提供する。

【解決手段】　料金所路側機13を通過する際、ＩＣカード11に記憶されたレスポンスデータ、すなわち料金所路側機13を通過した際に当該路側機13で生成した乱数(RND)がチャレンジデータとして車載機12経由でＩＣカード11に伝送され、それを正規の秘密鍵Ｋiccで暗号化したもの、が料金所路側機13に送信される。この際、ＩＣカード11のＩＤ(ICCID)とＩＣカード個別鍵証明書CERT－Ｋiccが共に送信される。路側機13では、送られてきたデータを３つに分割、すなわちレスポンスデータであるＥ(Ｋicc, RND)と、ICCIDと、ＩＣカード個別鍵証明書CERT－Ｋiccに分割する。次にＩＣカード個別鍵証明書CERT－Ｋicc を検証鍵PCに基づいて復号処理(ＤＥＣ)すると、ＫiccとICCIDという情報を取り出すことができる。このICCIDと、上記に分割して取り出したICCIDを比較してその一致判定を行ない、一致していればＩＣカードＩＤの署名確認を行なうことができる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社